REMARKS

Claims 1-25 were pending as of the action mailed on November 17, 2008. Claims 1, 5, 9, 14, 20, 24 and 25 are in independent form.

Claims 1, 5, 9-14, 20, and 24-25 are being amended. No new matter has been added. Support for the amendments can be found in the specification, for example, on page 9, line 27 to page 10, line 9; page 10, line 10 to page 11, line 22; and FIGS. 4A, 5, and 6.

Reconsideration of the action is respectfully requested in light of the foregoing amendments and the following remarks.

The Examiner rejected claims claim 24 under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. Patent No. 6,330,588 ("Freeman"). The Examiner rejected claims 1-23 and 15 under 35 U.S.C. § 103(a) as allegedly unpatentable over Jansen et al. "NIST Special Publication 800-19—Mobile Agent Security" ("Jansen") in view of U.S. Patent No. 6,233,601 ("Walsh") and Freeman. Applicant respectfully traverses the rejections.

Section 102 Rejection

Claim 24 is directed to a method that includes determining whether a first host has been designated as an untrusted host. When the first host is an untrusted host, code in the received jumping application that implements a particular behavior is replaced with a piece of code that implements the particular behavior in the jumping application so that the jumping application has the particular behavior when it is executed by the second host for each jump of the jumping application between hosts.

The Examiner states that Freeman describes replacing code of an untrusted hosts at col. 14, lines 7-18. Applicant respectfully disagrees. The cited portion of Freeman reads, in pertinent part, as follows:

> So implementing these mechanisms (and components) enables (a) the trusted resource to operate substantially protected from corruption and/or (b) the trusted resource's implicated mechanism(s) to be compared to, e.g., firmware copies from time to time so that, if any corruption is discovered, corrective measures can be invoked. Typical corrective measures include repairing software, e.g., by reloading objects, by deleting any extraneous code, by application of code

> comparison and correction algorithms or similar routines, and/or by other conventional approaches, whether automatically or by human initiation, such as by a system operator.

The cited portion of Freeman describes using a resource to verify mobile software agents. The verification identifies and detects corruption in the mobile agent to protect the mobile agent. The mobile agent can be corrected when corruption is identified. The correction includes repairing software by reloading an object, deleting code, and correcting code.

Thus, Freeman describes correcting the mobile agent when a corruption is identified. However, claim 24 requires that code be replaced from a jumping application when the first host has been designated as an untrusted host. Thus, whether the code is replaced is based on a property of the host, not the code.

Additionally, the Examiner asserts that if corrupted code is identified, than the host is considered an untrusted host. *See* Office Action at pages 7-8. Thus, the Examiner asserts that corruption of jumping application code is equivalent to whether a host is trusted or not. Applicant respectfully disagrees. The Examiner has not identified any portion of Freeman as indicating that corrupted code establishes a host as untrusted. In particular, the Examiner does not provide any evidentiary support at all for this conclusion. Applicant respectfully submits that this is not permissible under MPEP 2144.03. If the Examiner is attempting to take notice of the equivalence of code corruption and host trustworthiness, the Examiner is obliged to provide evidence in support of that conclusion. Moreover, when the Applicant challenges the Examiner's factual assertion, as occurred in the previous reply, the Examiner is required to support the finding with adequate evidence. *See* MPEP 2144.03(C).

In claim 24, the term "untrusted" refers to the host designation, not a property of the code. Thus, trust, as recited in claim 24, is a designation applied to the particular host and not the jumping application code.

Hosts and jumping applications are distinct and the designation of one does not teach or suggest the designation of the other. For example, a host can be designated as untrusted with or without having corrupted code in the jumping application. For example, any host outside a firewall may be identified as untrusted even though no corruption exists. Similarly, a trusted host can become infected, for example by a virus, that results in corrupted jumping application

code. Freeman, however, does not identify any issues of trust with respect to hosts. The Examiner has provided no support for the conclusion that host designations correspond to code content. Thus, the description of replacing corrupted code in Freeman does not teach whether or not the associated host has been designated as trusted or untrusted.

Moreover, claim 24 additionally requires that particular code is only identified for replacement when the host is designated as an untrusted host. To satisfy this requirement under the Examiner's interpretation, Freeman would have to identify corrupted code to cause a host to be designated as untrusted before identifying the corrupted code. Thus, claim 24 precludes corruption of code from being equivalent to the designation of a host as trusted or untrusted. Therefore, Freeman does not teach or suggest replacing code for an untrusted host as required by claim 24. Applicant respectfully submits that claim 24 is in condition for allowance.

Section 103 Rejections

Claim 1

Claim 1 was rejected over Jansen, Walsh, and Freeman. Claim 1, as amended, is directed to a jumping application security console that maintains the security of a jumping application that is jumping between two or more hosts connected to the security console though a network, the security console includes instructions to replace code from the jumping application when the jumping application is received at the security console during a jump between host, where the code is replaced for each jump of the jumping application between hosts.

The Examiner states that Jansen and Walsh do not teach the claimed replacing of code. Instead, the Examiner relies on Freeman as teaching the claimed replacing of code from the jumping application at col. 13, lines 35-50 and col. 14, lines 7-18. Applicant respectfully disagrees.

The portion of Freeman at col. 13, lines 35-50 reads as follows:

> A security mechanism provides for securing selected portions of the computing environment from corruption. The security mechanism can be variously implemented. As an example, the security mechanism can be implemented to process received agents, so as to protect one or more of the software agent, the origin resource, the destination resource and the trusted resource from any corrupting influences potentially present in the agent itself, regardless of the source (e.g., sourced incident to exercising the computing environment). Toward

> accomplishing that end, the security mechanism typically is enabled to remove, disable or otherwise render ineffective any or all of a received agent that may be corrupted or corrupting. Such a mechanism preferably includes monitoring firmware and/or other hardware which is used to identify agents and other potentially executable code that may be corrupted.

The cited portion describes a security mechanism that can be implemented to protect agents from corruption. In particular, the cited portion describes that the security mechanism can remove or disable part of a mobile agent that has become corrupted or is corrupting. The cited portion, however, does not teach or suggest replacing code **each** time a jumping application jumps between hosts, as required by claim 1.

Additionally, col. 14, lines 7-18 of Freeman reads, in pertinent part, as follows:

> So implementing these mechanisms (and components) enables (a) the trusted resource to operate substantially protected from corruption and/or (b) the trusted resource's implicated mechanism(s) to be compared to, e.g., firmware copies from time to time so that, **if** any corruption is discovered, corrective measures can be invoked. Typical corrective measures include repairing software, e.g., by reloading objects, by deleting any extraneous code, by application of code comparison and correction algorithms or similar routines, and/or by other conventional approaches, whether automatically or by human initiation, such as by a system operator. [Emphasis added]

The cited portion of Freeman describes using a resource to verify mobile software agents. The verification identifies and detects corruption in the mobile agent to protect the mobile agent. The mobile agent can be corrected **IF** corruption is identified. The correction includes repairing software by reloading an object, deleting code, and correcting code.

Thus, Freeman describes correcting the mobile agent only when a corruption is identified. However, claim 1 requires that code be replaced from a jumping application each time the jumping application jumps between hosts. Thus, code is replaced at each jump whether the code is identified as corrupted or not. If Freeman were to replace code each time, there would be no need to detect corruption. Thus, Freeman explicitly teaches against replacing code each time the jumping application jumps between hosts. Therefore, Freeman does not teach or suggest replacing code each time the jumping application jumps between hosts.

In responding to Applicant's prior arguments, the Examiner states "Freeman discloses returning to the trusted resource after every jump (column 6, lines 45-59). While at the trusted

resource the code is checked for correction and corrupted code is replaced" (Office Action page 8) (*emphasis added*). The Examiner fails to directly address the thrust of Applicant's previous argument, which is that Freeman only replaces code when it is identified as corrupted. However, the Examiner in arguing about whether or not the application returns to a trusted source each jump states that the code is checked and corrupted code is replaced. Thus, the examiner's own statement is in contrast with the requirement of claim 1 that code is replaced at every jump without any checking for corruption. Freeman's replacement under particular conditions does not teach or suggest the claimed replacing code for each jump of the jumping application between hosts.

Applicant respectfully submits that claim 1, as well as claims 2-4, which depend from claim 1, are in condition for allowance.

Claim 5

Claim 5 was rejected over Jansen, Walsh, and Freeman. Claim 5, as amended, is directed to a jumping application security console that includes replacing code from the jumping application that implements a first behavior with a piece of code from the database into the jumping application that implements the first behavior where the code is replaced during each jump between hosts.

As set forth above with respect to claim 1, the cited references do not teach or suggest replacing code of a jumping application when the jumping application is received at the security console during a jump between hosts and during each jump between hosts. Instead, Freeman describes replacing code only if a corruption is identified. Applicant respectfully submits that claim 5, as well as claims 6-8, which depend from claim 5, are in condition for allowance.

Claim 9

Claim 9 was rejected over Jansen, Walsh, and Freeman. Claim 9, as amended, is directed to a method that includes receiving the jumping application at the security console from a host; identifying a piece of code in the jumping application that implements a particular behavior; and removing the identified piece of code in the jumping application that implements the particular behavior each time the jumping application jumps between hosts. For at least the same reasons as set forth above with respect to claim 1, claim 9, as well as claims 10-13, which depend from claim 9, are in condition for allowance.

Claim 14

Claim 14 was rejected over Jansen, Walsh, and Freeman. Claim 14, as amended, is directed to a jumping application security system that includes instructions that replace code from the jumping application that implements a first behavior with a piece of code from the database when the jumping application is received at the security console during a jump between hosts, and where the code is replaced into the jumping application that implements the first behavior each time the jumping application jumps between hosts. For at least the same reasons as set forth above with respect to claim 1, claim 14, as well as claims 15-19, which depend from claim 14, are in condition for allowance.

Claim 20

Claim 20 was rejected over Jansen, Walsh, and Freeman. Claim 20, as amended, is directed to a server for a jumping application security system that includes instructions that replace code from a jumping application received from a host through a network with a piece of code from a database into the jumping application each time the jumping application jumps from the first host to a second host. For at least the same reasons as set forth above with respect to claim 1, claim 20, as well as claims 21-23, which depend from claim 20, are in condition for allowance.

Claim 25

Claim 25 was rejected over Jansen, Walsh, and Freeman. Claim 25, as amended, is directed to a jumping application security system that includes a security module having instructions to replace code from a jumping application with a piece of code from a database into the jumping application each time the jumping application jumps between hosts. As set forth above, the cited references do not teach or suggest replacing code ach time a jumping application jumps. Therefore, the cited references of Jensen, Walsh, and Freeman do not teach or suggest replacing code from a jumping application with a piece of code from a database into the jumping application each time the jumping application jumps between hosts. Applicant respectfully submits that claim 25 is allowable.

Conclusion

For the foregoing reasons, Applicant submits that all the claims are in condition for allowance.

By responding in the foregoing remarks only to particular positions taken by the Examiner, Applicant does not acquiesce with other positions that have not been explicitly addressed. In addition, Applicant's selecting some particular arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist. Finally, Applicant's decision to amend or cancel any claim should not be understood as implying that Applicant agrees with any positions taken by the Examiner with respect to that claim or other claims.

Please apply any credits or charges to Deposit Account No. 06-1050.

Respectfully submitted,

Date: March 16, 2009

/Brian J. Gustafson/
Brian J. Gustafson
Reg. No. 52,978

Customer No. 26181
Fish & Richardson P.C.
Telephone: (650) 839-5070
Facsimile: (650) 839-5071